Information Technology NEWS

Office of Information Technology

April 2005

Inside This Issue:

Charles W. Grim, DDS, MHSA
Director, IHS
Keith Longie, *CIO*
Wesley Old Coyote, *Deputy CIO*
Juan Torrez, *Editor*

New IHS Deputy CIO

I am pleased to announce the selection of Mr. Wesley Old Coyote, a member of the Crow Tribe, as the Deputy Chief Information Officer of the Office of Information Technology (OIT) for the Indian Health Service (IHS). Wes will be responsible in assisting me with the operations of the OIT.

Mr. Old Coyote previously served as the Chief Information Officer of the Navajo Area Indian Health Service (NAIHS) Information Resource Management (IRM) department from May 2002 to Mar 2005. The Navajo Area IHS includes six Federal service units, three Tribal corporations and one Urban program supporting a broad range of Digital Information Systems resources, telemedicine activity, administrative and clinical operations, telecommunications infrastructure development and implementation, policy implementation, and strategic planning.

After a career in the US Navy, Mr. Old Coyote joined the IHS in 2001, as the Chief Information Officer of the Navajo Area IHS. In FY 2002, he transferred to the Phoenix Area IHS, where he worked as the Supervisor of the Information Resource division in the Office of Planning, Evaluation and Information Resources. In May 2002, he returned to the Navajo Area IHS, where he continued with the development of the NAIHS Telehealth and Telemedicine network infrastructure. In FY 03/04, Mr. Old Coyote performed IHS-wide systems infrastructure assessments in support of the Electronic Health Record (EHR) and telemedicine implementation projects.

Mr. Old Coyote holds a Bachelor of Science in Business Administration from the University of La Verne, and numerous Information Systems certifications and qualifications from the US Navy.

Please join me in welcoming Wes in his new capacity. ■

Keith Longie
IHS Chief Information Officer

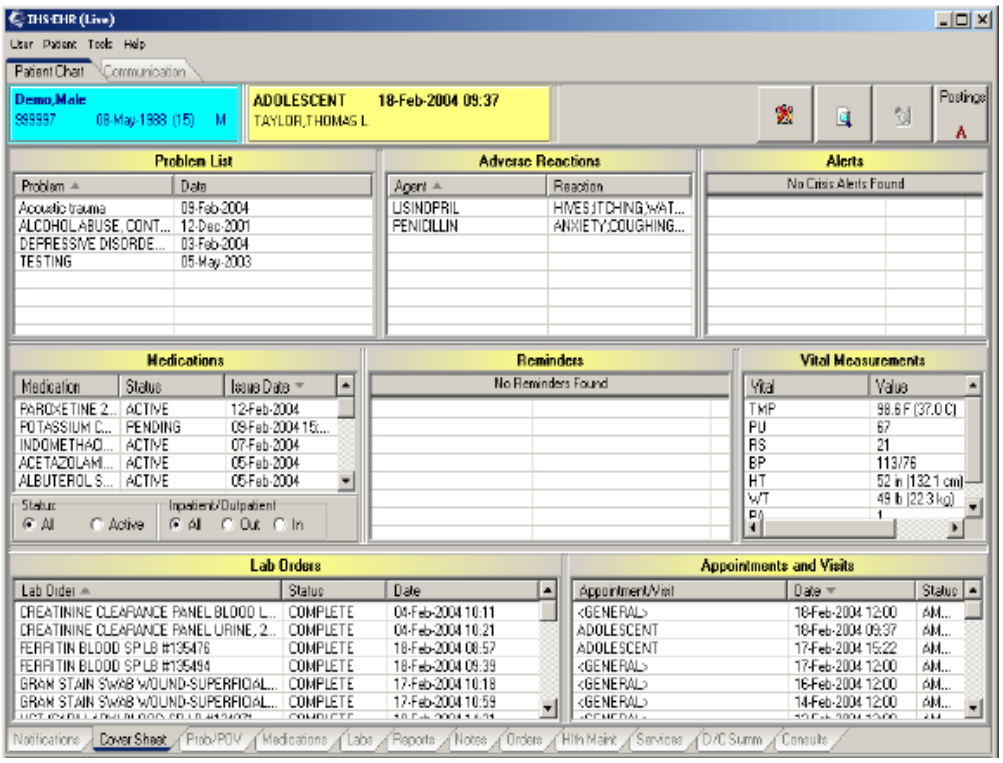
Tech Conference Announced

The IHS Information Technology Conference is right around the corner. This year's conference will be held in Scottsdale, Arizona on the week of June 27, 2005 pending approval of the department. The theme of this year's conference is "Raising Indian Health Through Information Technology". As always, the conference promises to be filled with many fascinating seminars and presentations from people throughout the IHS in addition to outside vendors. Watch the IHS Web site for more specific information as it develops. ■

Bruce Parker, *Acting Director*
Division of Resource Management

EHR Approved For Deployment

Effective January 21, 2005, the IHS Electronic Health Record graphical user interface (GUI) was certified as an official RPMS software application. The IHS EHR Program wishes to express its sincerest appreciation to the leadership and staff of the following facilities who participated in beta testing EHR:



Wind River Service Unit, WY
Crow Indian Hospital, MT
Warm Springs Health and Wellness Center, OR
Cherokee Indian Hospital, NC
WW Hastings Indian Hospital, OK
Gila River Health Center, AZ
Fort Defiance Indian Hospital, AZ

At least a hundred clinical users and numerous support staff are using EHR for day-to-day patient care at these and other facilities — many of these users have more than a year of experience with EHR. Their valuable insights and feedback have contributed to past and future improvements to the application.

Several additional facilities have joined the beta test sites in using EHR for patient care, so that in mid-March the number of EHR sites has risen to fifteen. Numerous others are at various points along the implementation pathway.

Because of the profound clinical and business process changes forced by implementation of an electronic medical record, and the impact upon multiple departments in a facility, a lead-in period of at least 9-12 months is recommended to prepare for EHR. For this reason, release of the two major EHR-related software suites (Pharmacy/Order Entry and the EHR Graphical User Interface) is being controlled by the Office of Information Technology (OIT) in Albuquerque. The software can be released to, and OIT will support, only those facilities who have met a number of prerequisites for installation and staff preparation.

Facilities interested in entering the queue for EHR implementation should visit the "Preparing for EHR" page on the EHR Web site (www.ihs.gov/cio/ehr). This page provides a number of documents, including a self-assessment survey which can be submitted to the EHR Program as notification of intent to pursue EHR.

A new series of EHR training sessions has been launched. Week-long training events for Clinical Application Coordinators (CAC) and implementation teams are being held bi-monthly, and advanced CAC training sessions have begun as well. A variety of other specialty-oriented EHR training sessions (such as for technical staff, pharmacists, medical records, etc.) are also being designed.

Access to most of the formal EHR training events is restricted to staff from facilities that have accomplished certain milestones in EHR preparation, such as implementation of Pharmacy 5/7. However, the Warm Springs and Cherokee facilities have developed one-day EHR Overview courses that are suitable for representatives from facilities that are just getting started and want to see EHR in practice and what the future holds for them. Links to registration for these training events can be found on both the EHR and OIT Training Web sites.

EHR development is ongoing. Two patches are scheduled for release in April and May, and programming for version 1.1 is underway with release anticipated in the mid-summer. In addition, programming changes to a number of RPMS applications are taking place in order to resolve several issues contributing to an increase in PCC errors at EHR sites. Longer term plans include a major upgrade in EHR functionality with the completion of EHR version 2.0 early in 2006. ■

Howard Hays, MD, MSPH,
IHS-EHR Program Director

Division of Information Security News

Use Care When Reading E-mail with Attachments

You probably receive lots of mail each day, much of it unsolicited and containing unfamiliar but plausible return addresses. Some of this mail uses social engineering to tell you of a contest that you may have won or the details of a product that you might like. The sender is trying to encourage you to open the letter, read its contents, and interact with them in some way that is financially beneficial – to them. Even today, many of us open letters to learn what we've won or what fantastic deal awaits us. Since there are few consequences, there's no harm in opening them.

E-mail-borne viruses and worms operate much the same way, except there are consequences, sometimes significant ones. Malicious e-mail often contains a return address of someone we know and often has a provocative Subject line. This is social engineering at its finest – something we want to read from someone we know.

E-mail viruses and worms are fairly common. If you've not received one, chances are you will. Here are steps you can use to help you decide what to do with every e-mail message with an attachment that you receive. You should only read a message that passes all of these tests.

1. The **Know** test: Is the e-mail from someone that you know?

2. The **Received** test: Have you received e-mail from this sender before?

3. The **Expect** test: Were you ex-

continued on page 11

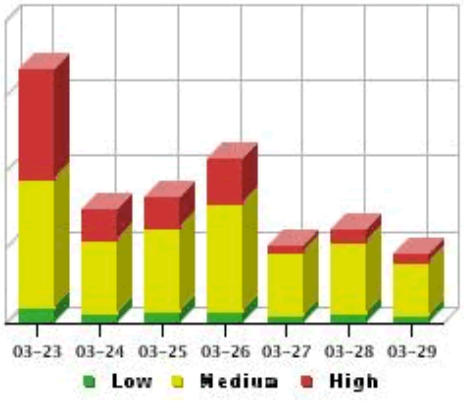
Intrusion Detection Sensors (IDS)

The IHS IDS analyzed 1,182,522 potentially malicious attacks/events from March 23rd through March 29th.

To the right, there are two graphs: one illustrates the number of attacks/events registered from March 23rd through March 29th by the IHS IDS and the other illustrates the number of attacks/events registered during that same period worldwide.

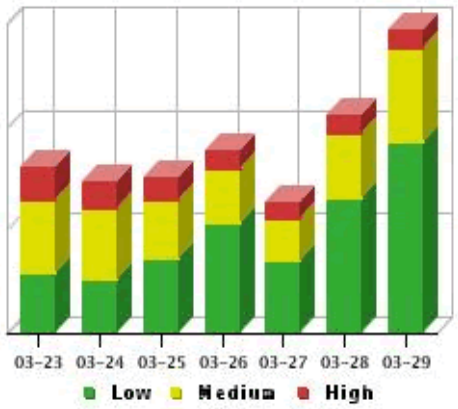
While this number is quite large, the count includes many attempts by old viruses that are getting through to IHS systems. These could be easily prevented with the proper anti-virus software. Anti-virus software should be continually updated and set to auto scan. In addition to updated anti-virus software, systems should also have the latest updates and fixes for all software installed.

System administrators should always update and patch all computer systems (desktops, laptops, servers, etc.), including systems that are rarely used or those which are not currently, but potentially could be, connected to the network.



IHS IDS Event Trend

IHS sensors analyzed 1,182,552 potentially malicious attacks from March 23rd to March 29th



Global IDS Event Trend

Global network of customer sensors have analyzed 126,605,643 potentially malicious attacks from March 23rd to March 29th

Kathleen Federico, *Assistant ISSO*

Clinical Reporting System (CRS) Update

CRS 2005 Software

The Clinical Reporting System (CRS, formerly known as GPRA+) 2005, Version 5.0 software was nationally released on October 21, 2004. Key changes for this version include:

- New National GPRA report (replaces the GPRA Performance and Area Director Performance reports). This report will be used for quarterly and annual GPRA reporting. It automatically selects American Indian/Alaska Natives as population, report period July 1, 2004 - June 30, 2005, and 2000 as baseline year.
- Revised CVD and Cholesterol Screening and Prenatal HIV Testing to GPRA indicators.
- Five new indicator topics:
  - Childhood Immunizations (GPRA indicator for 2005)
  - Childhood Obesity Reduction (proposed GPRA indicator for 2006)
  - Chronic Kidney Disease Assessment
  - Comprehensive CVD-Related Assessment for At-Risk Patients
  - Diabetes Comprehensive Care
- New option to print Patient Lists for patients who meet or do not meet indicators included in the National GPRA report.

Patch 1 for this software was released on January 31, 2005. Key features included in the patch are:

- Change to Diabetes: Nephropathy Assessment GPRA indicator that removes requirement for an Estimated GFR test.
- Added logic now requiring users to have security keys to run patient lists, edit site parameters, and edit site-defined taxonomies.
- Added new report (GPU option from Other National Reports menu) that enables users to run the same indicators included in the National GPRA report but for a report period they specify.

Development of CRS Version 5.1 is underway and beta testing is anticipated to begin the end of April, with national release by the end of May. Key changes for this version include:

- New CMS report, includes 10 quality measures for heart attack, heart failure, and pneumonia

continued on page 11

IT Security Awareness Tip

With the development of the CD burner, software licensing is increasingly becoming an issue. Instead of purchasing the software, people are making copies of them, which is in violation of many licenses. To protect the interest of the Department, all personnel should ensure that their daily activities comply with software licenses. This includes ensuring that software is properly licensed before being installed on the Departmental system and that the software is used in its intended manner.

Please remember that it is prohibited to do the following:

- Copy or distribute software or its accompanying documents and applications without permission from the copyright owner
- Encourage, allow, compel, or pressure others to make or distribute unauthorized software copies
- Loan software for duplication
- Remove any technical means applied to protect the software program, including the creation or possession of articles intended to facilitate deletion
- Modify software without proper approval from your OPDIV's Information Systems Security Officer (ISSO)
- Use personally owned software to process, access, or store Departmental information without written authorization from the OPDIV Chief Information Security Officer (CISO)

In addition, please complete the following:

- Activate security features and controls when processing Departmental information
- Notify the ISSO of any misuse of Departmental software or the use of personnel software without CISO permission

Kathleen Federico, *Assistant ISSO*

Business Office News

HIPAA Transactions Workgroup to Receive IHS Directors Award

In an effort to actively recognize our end users for their ongoing support with RPMS initiatives, the Office of Information Technology submitted a nomination form for the HIPAA Transactions Workgroup to the Indian Health Service Director Awards Committee. Happily, we are able to report that the workgroup was approved and will be one of the groups receiving recognition at the IHS Director's Award Ceremony to be held on April 22, 2005 in Bethesda, MD.

The workgroup was submitted for outstanding work by implementing HIPAA compliant Transactions and Code Sets in support of the RPMS software and third party revenue operations.

Details of the work involved are as follows: Implementing HIPAA compliant Transaction and Codes Sets have been a top priority for I/T/U facilities. A major challenge of this task was ensuring the I/T/U supported RPMS software was in compliance with all transactions and code sets based on multiple third party requirements. To accomplish this task, ongoing support, testing and guidance was provided by a multi-tiered team consisting of Service Unit Business Office staff, Service Unit Site Managers, Area Business Office Coordinators and Office of Information Technology support staff. Daily communication including bi-monthly conference calls were ongoing to provide networking on a national level as well as identify major issues not only related to the software but also business process changes, contracting issues and payer issues. The diligent work provided by this workgroup not only assisted multiple I/T/U facilities with continuous third party revenue but increased the success rate of I/T/U facilities of being HIPAA compliant with Medicare by 95% in FY 2004. This group has been in existence for well over a year and continues to work as a team to address issues as they arise.

The work group included the following people:

CDR Sandra M Lahi, Mgmt Analyst, OIT;

Adrian Lujan, User Support Specialist, OIT;

Carl Gervais, Computer Analyst, OIT;

Margaret Bahr, Site Manager, Red Lake Hospital, Bemidji Area;

David Battese, IT Specialist, Portland Area;

Lauren Folson, Lead Biller, Sells SU, Tucson Area;

Toni Johnson, IT Specialist, California Area;

Violet Kenny, IT Specialist, Phoenix Area;

Cynthia Larsen, Business Office Coordinator, Billings Area;

Charolett Melcher, IT Specialist, Phoenix Area;

Kurt Priessman, Tucson Area;

Sharon Sorrell, Business Office Manager, GIMC, Navajo Area;

Brenda Tahe, Lead Biller, GIMC, Navajo Area;

Jan Thunder, Business Office Manager, Red Lake Hospital, Bemidji Area;

Roland Todacheenie, Business Office Coordinator, Navajo Area;

Gail Townsend, IT Specialist, Albuquerque Area;

David Walton, IT Specialist, Sells SU, Tucson Area.

Special recognition must also be made to Art Gonzales, Elmer Brewster, Catherine Thompkins, Dyanne Leyba, Shonda Render, Linda Lehman, Lisa Jaramillo, Pam Schweitzer, Raymond Willie, and George Huggins for their efforts in this initiative.

Congratulations to the group for a job well done and keep up the good work! ■

Sandra Lahi
Management & Program Analyst

Emergency Room System (ERS)

Status Update

The Emergency Room System Workgroup (ERSWG) began meeting in January 2005 to discuss ERS issues and concerns. The workgroup, composed of ER providers, is led by Dr. Allen Dobbs, Chief of Emergency Medicine at Phoenix Indian Medical Center (PIMC)

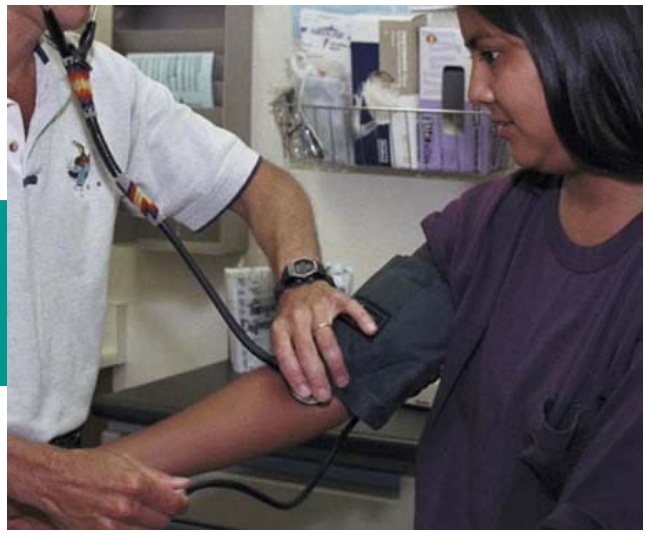
The ERSWG is committed to promoting and guiding further development of the ERS application, which will facilitate a higher level of emergency patient care and patient data management. The workgroup will hold a monthly conference call with the goal of developing a prioritized list of recommendations and requirements to enhance the existing software. Requirements identification is the first step to the creation and deployment of a new ERS patch in CY05.

Currently, ERS v2.5 allows you to register, admit, and discharge patients from the ER. It also allows you to run a broad range of reports that help you view and manage the flow of patients and the staff workload.

The monthly conference call is held every 3rd Thursday of the month at 10:00 am Mountain time. The workgroup is planning to have a face-to-face meeting during Spring 2005 to finalize the enhanced functional requirements.

If you have any suggestions or issues that the workgroup should consider regarding the Emergency Room System or if you have any questions, please contact Joann Jaramillo at Joann.Jaramillo@ihs.gov. ■

Joann Jaramillo
User Support



Women's Health (WH) Package

Status Update

The Women's Health package (WH) v3.0 is in the beginning phases of development. Currently, WH v2.0 identifies and tracks women's Pap smear tests and/or colposcopy; tracks exams and results and suggest actions and follow-up based on results; and provides epidemiological, workload, treatment and pregnancy due reports. Version 3.0 is intended to expand the capabilities of v2.0 to include tracking of family planning strategies and outcomes and osteoporosis risk factors.

Facilitating this development is the Women's Health Requirements Workgroup (WHRWG). The workgroup is led by Dr. Theresa Cullen and comprised of approximately 10 clinicians, as well as members of the Clinical Applications Team (CAT). Convening in Phoenix, Arizona on March 16 and 17, the WHRWG will work to develop the requirements for WH v3.0. The workgroup has an aggressive timeline for development with a goal to release v3.0 in late CY 2005.

The Women's Health package is one of many applications slated to be a part of the Integrated Case Management (ICM) structure. ICM will function as a framework from which multiple individual case management applications, such as Women's Health, Diabetes Management, and Asthma Management will be accessed. A major benefit to this framework will be the ability to enter patient information in multiple case management applications without having to switch between those applications. ICM will also enable Case Managers to view all the patient data entered in the various case management applications on one screen, as well as perform consolidated reporting of patient's registered in more than one application. Sites will still have the option of installing only the case management applications they use.

The WHRWG is committed to providing the guiding force to further develop the WH application and ensure its consistency with established case management standards. The workgroup will develop additional requirements that will improve the quality of care delivered to our female patients.

If you have any suggestions or questions regarding the Women's Health v3.0 enhancements, please contact Joann Jaramillo Joann.Jaramillo@ihs.gov as soon as possible. ■

Joann Jaramillo
User Support

UDS 2004 Software

The Uniform Data System (UDS) 2004, Version 2.0 software was released nationally on January 5, 2005. RPMS UDS reporting is intended for use by tribal or urban health facilities receiving grant funds for primary care system development programs administered by the Bureau of Primary Health Care (BPHC), Health Resources and Services Administration (HRSA). The RPMS UDS Reporting System provides passive extraction of patient and visit data from the IHS Resource and Patient Management System (RPMS) to produce four of the nine UDS reports. For each of the four reports, RPMS UDS also produces lists of all patients and related visits that are counted in the reports.

This version included changes to the format and logic for Table 5, *Staffing and Utilization* and Table 6, *Selected Diagnoses and Services Rendered*, as required by BPHC, and changes to the definition of encounters for all RPMS visits. Section 1.1 of the UDS User Manual contains a complete list of changes.

UDS reports were due to BPHC on or before February 15, 2005 for calendar year 2004. ■

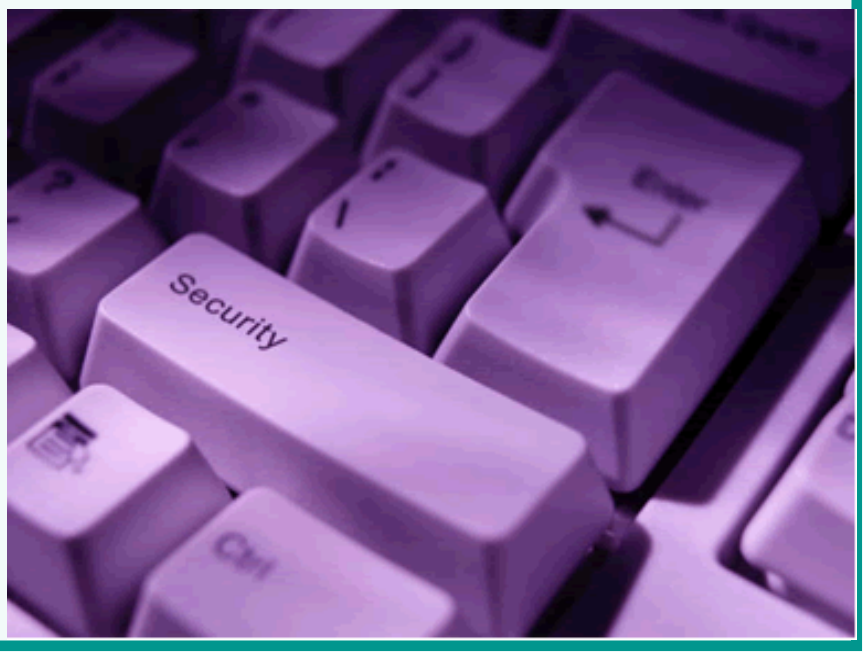
Stephanie Klepacki
CRS Project Coordinator

Theresa Cullen, MD, MS
National Medical Informatics Consultant

IT Security Awareness Tip
Safe Telecommuting Practices

As telecommuting becomes a more viable option for getting work done, it is important to remember that maintaining good security practices when telecommuting is just as important as maintaining good security practices when you work in the office. To ensure the protection of the Department's hardware and software from theft, damage, or misuse while working outside the office, to the following safe practices are recommended:

- Ensure anti-virus software is installed and virus definitions are updated regularly
- Store sensitive data on your system only if your system is encrypted
- Send sensitive data only if it is encrypted
- Report lost or stolen equipment, security incidents, or anything unusual immediately to the appropriate ISSO
- Provide a secure and protected environment for HHS data and HHS-owned computing resources from unauthorized disclosure or damage
- Perform actions that are compliant with HHS or federal regulations and policies
- Contact the Office of Security and Drug Testing (OSDT) for information considered Classified Data



Please remember that everyone is responsible for the confidentiality and integrity of any information on his/her system.

Kathleen Federico, *Assistant ISSO*

RPMS Development News

Recent Releases

Periodic Releases
Average Wholesale Pricing (APSA) v6.1 patch 58
CPT Current Procedural Terminology (ACPT) v2005 and v2005 Patch 1
IHS Standard Table (AUM) v5.1 patch 5
IHS Pharmacy Mods (APSP) v7.0 patch 2
Patient Drug Education (APSE) v6.10 patch 19
VA Clinical Reminders (PXRM) v1.5 patch 1001
VA Patient Care Encounter (PX) v1.0 patch 1001

ARMS (ACR) v2.1 patch 15
Removed modification made to comply with TFM Bulletin 2004-06 that requires Federal agencies to submit their vendor and miscellaneous bulk payment files specifying those payments that are subject to Offset through the Treasury Offset Program (TOP). Travel Payments are not exempt.

Clinical Reporting System (BGP) v5.0 patch 1
Patch 1 of Clinical Reporting System version 5.0 makes the following changes: added security keys to the System Setup menu to edit the site parameters option, select/edit site-defined taxonomies option, and all reports; revised numerator for Diabetes GPRA indicator; added separate report option that enables users to run the National GPRA report for any report end date or ending on a predefined quarter; enabled users to select report Current Report Period date range when running National GPRA patient lists; added "Area Current" column to the Area Aggregate National GPRA report, Clinical Detail Section; added separate Area Office report option that enables Area Office users to run an Area Aggregate GPRA Performance report.

Diabetes Management System (BDM) v1.0 patch 5
Patch 5 makes 13 fixes and modifications to v1.0. These changes increase the programs usability, functionality, and ability to meet 2005 audit criteria.

Patient Information Management System v5.3 Patch 1
PIMS v5.3 Patch 1 was released on January 11, 2005. The patch includes fixes for a host of issues identified since its release in July 2004. Modifications affect both, the Scheduling and Admit/Discharge/Transfer (ADT) modules. Within ADT, changes have been made to Admission Form, Day Surgery, Patient Admission, Patient Inquiry, Observation Patient, and Report functions. Scheduling module changes affect the Clinic Setup, Routing Slips, Chart Requests, and Multiple Appointment Booking functions.

Patient Registration (AG) v7.0 patch 5
Patch 5 adds a utility to search through a database's Patient file and determine whether fields are missing data or have incorrectly formatted data in preparation for the installation of version 7.1. Sites can run the audit report and then correct improper data before installation of 7.1. The file produced from the audit will contain data for all sites on which the database is being run. A new list of error and warnings was also added so that the registration clerk may be able to quickly identify and correct any identified problems.

PCC Health Summary (APCH) v2.0 patch 12
Patch 12 makes several fixes and modification to the APCH package including: modified In-Hospital section of the health summary; modified EXAM section; added new component called Radiology Exams; 5 modifications to the Diabetes Supplement; added new Pre Diabetes Care Summary as a supplement type; added new component for Education Assessment which displays Health Factors; added LOINC code lookup; added ability to automatically switch from the health summary type defined by the clinic in scheduling to the diabetes summary type if the patient has diabetes on the problem list or has had a diagnosis of Diabetes on a visit with a primary care provider; modified allergy sections of the health summary to work with both the new and old versions of allergy tracking; added new component for scheduled encounters that excludes chart requests and walk ins; added a new health maintenance reminder for DOMESTIC VIOLENCE/IPV SCREENING the criteria is to prompt for Due every year for females 15 and over; and added 2 medication reorder documents.

Pharmacy Auto Refill System (BEX) v1.0 patch 01
This patch adds fixes for PIMS v5.3 and Pharmacy v7 and additional site parameter for PM Routing Slip Printer.

Pharmacy Point of Sale (ABSP) v1.0 patch 11
The primary purpose of this patch is to provide the claim format for the new Medicare pharmacy card, effective within IHS July 1, 2004. In addition, a few claim formats have been adjusted to match current processor requirements.

continued on page 12

The IHS completes the transition to vBNS+

The IHS has converted all of its FTS 2001 implemented circuits to MCI's vBNS+ service as part of the transition to HHSNET. The number of circuits is listed below:

- T1 connections - 105
- Frame Relay - 193

The MCI vBNS+ network was launched in 1995 as a collaborative effort between MCI and the U.S. National Science Foundation. It was initially created as a US nationwide network that supported high-performance, high-bandwidth research applications. At that time it was known as the very high-speed Backbone Network Service (vBNS).

The collaborative research effort was completed in 2000 when the project evolved into the commercial offering now known as vBNS+. This Internet Protocol (IP) network is constructed from Juniper Networks' routers driving OC-48 and OC-192 trunks.

Because it is a commercial network, the vBNS+ network is an unclassified network, and it employs controls that ensure the confidentiality, availability, and integrity of the network services in accordance with this designation. However, it should be noted that classified U.S. Government information can be transmitted across the vBNS+ network provided that it is **"properly encrypted by the customer"** prior to entering the network as U.S. Government policy dictates.

The customer has a layer-3 (IP) connection to the vBNS+ network; however, the customer data is forwarded across the network using MPLS. Multi-Protocol Label Switching (MPLS) is a packet-forwarding protocol for directing a flow of protocol-independent data units, in this case Internet Protocol (IP) packets, along a predetermined path across a network.

The Office of Information technology is currently working on an IHS-wide contract that will provide routers with the necessary encryption for the IHS vBNS+ network. ■

Tom Fisher
Acting Director, Division of Enterprise Project Management

IHS Active Directory Migration Update

Seventy-five sites have currently migrated to the Active Directory with forty-four sites remaining. While the migration is proceeding slowly, the OIT continues to seek funding and schedule conversions. The Technology Management Team is working closely with the Active Directory technicians to assure quality installations that meet the IHS requirements.

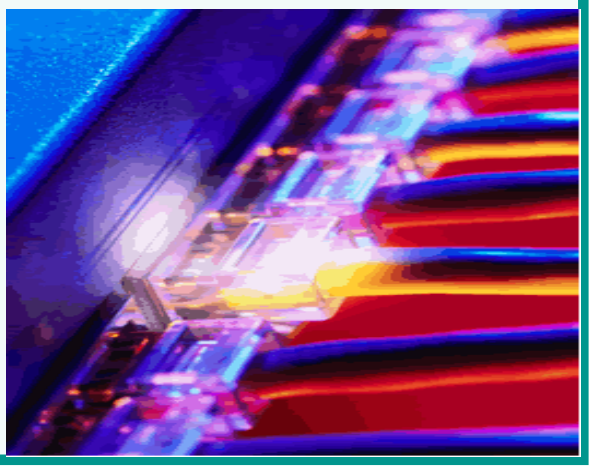
This is considered one of the important "OneHHS" initiatives for IHS as we prepare for e-mail consolidation. If your site has not yet converted to Active Directory, please contact Mr. Michael Becker of Dell Professional Services at (301) 983-1441 to schedule your migration. ■

Karen Wade
Computer Specialist

Help Desk Statistics

The OIT Help Desk closed 1464 support calls for the fourth quarter.
Here's a breakdown of those calls:

1. Resolved within 0-7 Days: 781 (54%)
2. Resolved within 8-14 Days: 151 (10%)
3. Resolved within 15-21 Days: 58 (4%)
4. Resolved within 22+ Days: 474 (32%)



You can contact the OIT Help Desk by:
Phone: 888-830-7280 or 505-248-4371
or **E-Mail:** ITSCHelp@IHS.HHS.gov

Alex Fullam, *User Support Specialist*

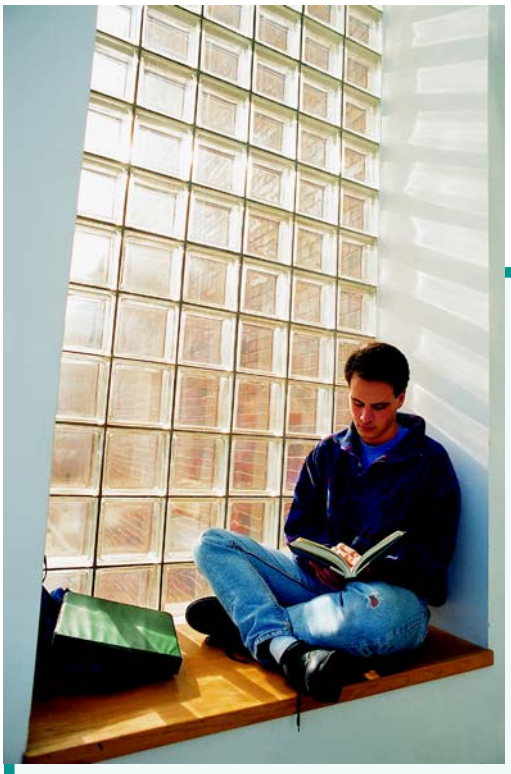
RPMS Training Schedule

OIT Sponsored Training

The following trainings are sponsored by the Office of Information Technology (OIT):

April

04/5-7	RCIS - Albuquerque
04/5-7	PCC Outputs – Tucson
04/5-6	Behavioral Health GUI – Oklahoma
04/7-8	Behavioral Health GUI - Oklahoma
04/12	Emergency Room Package – Billings
04/12-14	Radiology v5.0- Aberdeen
04/18-22	EHR CAC Trainings- Albuquerque
04/18-22	PCC Data Entry I & II – Oklahoma
04/19-20	Behavioral Health – Nashville
04/19-21	PCC+ - Aberdeen
04/19-21	Site Manager- Bemidji
04/19-21	PIMS – Phoenix



May

05/3	Emergency Room System – Albuquerque
05/3-4	POS Pharmacy Billing – Oklahoma
05/3-5	PCC+ - Navajo
05/9-13	PCC Data Entry – Portland
05/10-11	Behavioral Health v3.0 – Bemidji
05/10-12	PCC Outputs – Nashville
05/10-12	Intermediate Laboratory – Albuquerque
05/12-13	Behavioral Health GUI – Bemidji
05/17-19	EHR for HIM and Business Office –Albuquerque
05/17-19	Site Manger – Billings
05/17-19	Advanced Third Party Billing/ AR- California
05/24-25	Behavioral Health Reports & Manager Utilities – Albuquerque
05/24-26	Patient Registration V7.1 – Aberdeen

June

06/1-3	Basic Site Manger – Little River Casino and Resort, Manistee, MI
06/1-3	Radiology v5.0 – Phoenix
06/6-10	PCC Data Entry I & II – Navajo
06/7-8	Behavioral Health Reporting – Phoenix
06/7-8	POS Pharmacy Billing - Bemidji
06/7-9	Patient Registration v7.1 – California
06/9-10	Behavioral Health GUI - Tucson
06/14-16	PCC Outputs – California
06/14-16	Advanced Third Party Billing/ Accounts Receivable – Phoenix
06/20-24	EHR CAC & Implementation Team – Albuquerque
06/21-23	Introduction to Laboratory – Oklahoma
06/21-23	Patient Registration – Oklahoma
06/28-30	Basic Site Manager – Oklahoma

If you are interested in attending any of the OIT sponsored trainings please visit the OIT National Training Web page at: http://www.ihs.gov/Cio/RPMS/index.cfm?module=Training&option=index

or contact:

Michelle Riedel
RPMS Training Coordinator
(505) 248-4446
Michelle.Riedel@IHS.HHS.gov

Area Sponsored Training

If you would like your Area trainings to be included in this publication, please contact the IT News.

Division of Information Security

continued from page 3

pecting e-mail with an attachment from this sender?

4. The **S**ense test: Does e-mail from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense? For example, would you expect the sender – let's say your Mother – to send you an e-mail message with the Subject line "Here you have, ;o)" that contains a message with attachment – let's say AnnaKournikova.jpg.vbs? A message like that probably doesn't make sense. In fact, it happens to be an instance of the Anna Kournikova worm, and reading it can damage your system.

5. The **V**irus test: Does this e-mail contain a virus? To determine this, you need to install and use an anti-virus program.

You should apply these five tests – **KRESV** – to every piece of e-mail with an attachment that you receive. If any test fails, toss that e-mail. If they all pass, then you still need to exercise care and watch for unexpected results as you read it. Now, given the **KRESV** tests, imagine that you want to send e-mail with an attachment to someone with whom you've never corresponded – what should you do? Here's a set of steps to follow to begin an e-mail dialogue with someone:

1. Since the recipient doesn't already **K**now you, you need to send them an introductory e-mail. It must not contain an attachment. Basically, you're introducing yourself and asking their permission to send e-mail with an attachment that they may otherwise be suspicious of. Tell them who you are, what you'd like to do, and ask for permission to continue.

2. This introductory e-mail qualifies as the mail **R**eceived from you.

3. It is to be hoped that they'll respond; and if they do, honor their wishes. If they choose not to receive e-mail with an attachment from you, don't send one. If you never hear from them, try your introductory e-mail one more time.

4. If they accept your offer to receive e-mail with an attachment, send it off. They will **K**now you and will have **R**eceived e-mail from you before. They will also **E**xpect this e-mail with an attachment, so you've satisfied the first three requirements of the **KRESV** tests.

5. Whatever you send should make **S**ense to them. Don't use a provocative Subject line or any other social engineering practice to encourage them to read your e-mail.

6. Check the attachments for **V**i**ruses**. This is again based on having virus-checking programs, and we'll discuss that later.

The **KRESV** tests help you focus on the most important issues when sending and receiving e-mail with attachments. Use it every time you send e-mail, but be aware that there is no foolproof scheme for working with e-mail, or security in general. You still need to exercise care. While an anti-virus program alerts you to many viruses that may find their way to your home computer, there will always be a lag between when a virus is discovered and when anti-virus program vendors provide the new virus signature. This means that you shouldn't rely entirely on your anti-virus programs. You must continue to exercise care when reading e-mail. ■

Ginn, Arnold "Mike"
Computer Specialist

CRS Dev.

continued from page 4

- 6 new indicators (also included in HEDIS report):
  - Topical Fluoride (GPRA indicator for 2005)
  - 3 CVD-related
  - Osteoporosis Management in Women
  - Asthma Quality of Care
- New Elder Care report (patients 55+)
- New Graphical User Interface (GUI)
  - Windows-based
  - Will be in addition to current roll-and-scroll

CRS 2005 Training

Two types of CRS training were offered this year: a class providing an overview of GPRA, PART, and CRS and a CRS Hands-on Training class. Training has been conducted at 11 Area Offices and concludes in mid-June. Training materials are available online at http://www.ihs.gov/cio/crs/crs_fy05.asp.

GPRA Quarterly Reporting

Quarterly GPRA reporting began in February, and the next quarterly reports are due from the Area Offices to California Area (carol.goodin@ihs.gov) by Tuesday, April 26, 2005. The CRS software will be used for all GPRA reporting. Instructions for both site and Area Office reporting are available at the CRS Web site at http://www.ihs.gov/cio/crs/crs_reporting.asp. ■

Stephanie Klepacki
CRS Project Coordinator

Theresa Cullen, MD, MS
National Medical Informatics Consultant

continued from page 8

Referred Care Information System (BMC) v3.0 patch 1
RCIS patch 1 makes 9 changes to v3.0, including changes to the General Retrieval Report, new menu options and letters, improved printing capability, and improvements to functionality.

Third Party Billing (ABM) v2.5 patch 7
Third Party Billing v2.5 Patch 7 contains (please note: this patch is only needed for EHR sites) a change to the claim generator. If the visit is inpatient and the clinic is pharmacy, the clinic will be changed to general.

Uniform Data System (BUD) v2.0
RPMS UDS Reporting is intended for use by tribal or urban health facilities receiving grant funds for primary care system development programs administered by the Bureau of Primary Health Care (BPHC), Health Resources and Services Administration (HRSA). The RPMS UDS Reporting System provides passive extraction of patient and visit data from the IHS Resource and Patient Management System (RPMS) to produce four of the nine UDS reports. For each of the four reports, RPMS UDS also produces lists of all patients and related visits that are counted in the reports.

VA Text Integration Utility (TIU) v1.0 patch 1001
Patch 1001 makes the following modifications to Text Integration Utility: fixed 3 known errors; added 2 new codes; added ability for sites who are using CIA code to upload documents; added ability for sites running VA Consults and VA Problem List to link documents; added hidden actions to SSD and MPD options; and added 17 new objects. ■

Carl Gervais
Computer Analyst

Contributors

Theresa Cullen, MD
(520) 670-4803
Theresa.Cullen@IHS.HHS.gov

Kathleen Federico
(505) 248-4381
Kathleen.Federico@IHS.HHS.gov

Tom Fisher
(505) 248-4219
Tom.Fisher@IHS.HHS.gov

Alex Fullam
(505) 248-4231
Alex.Fullam@IHS.HHS.gov

Carl Gervais
(505) 248-4197
Carl.Gervais@IHS.HHS.gov

Arnold "Mike" Ginn
(505) 248-4787
Arnold.Ginn@IHS.HHS.gov

Howard Hays, MD
(602) 263-1687
Howard.Hays@IHS.HHS.gov

Joann Jaramillo
(505) 248-4160
Joann.Jaramillo@IHS.HHS.gov

Stephanie Klepacki
(505) 821-4480
Stephanie.Klepacki@IHS.HHS.gov

Sandra Lahi
(505) 248-4206
Sandra.Lahi@IHS.HHS.gov

Keith Longie
(301) 443-8680
Keith.Longie@IHS.HHS.gov

Bruce Parker
(505) 248-4360
Burce.Parker@IHS.HHS.gov

Michelle Riedel
(505) 248-4446
Michelle.Riedel@IHS.HHS.gov

Christy Tayrien
(918)336-4181
Christy.Tayrien@IHS.HHS.gov

Karen Wade
(505) 248-4254
Karen.Wade@IHS.HHS.gov

David White
(505) 248-4190
David.White@IHS.HHS.gov

About the IT News

The IT News is published several times throughout the year by the IHS Office of Information Technology. All articles and article suggestions are gladly accepted. If you would like to submit an article for consideration or have any questions regarding this publication please contact Juan Torrez at (505) 248-4355 or Juan.Torrez@IHS.HHS.gov.

All articles should be no longer than 1200 words in length and be in an electronic format (preferably MS Word). All articles are subject to change without notice.